International Journal of Predictive Insurance Accounting and Management Sciences | ISSN *pending*
Published by NEXPUB

The Adoption of Advanced Cyber Laws as an Effort to Curb Internet Fraud in Nigeria

Egiyi, Modesta Amaka
Department of Accounting
Godfrey Okoye University

Publication Process	*Date*
Received	***September 16, 2020***
Accepted	***September 28, 2020***
Published	***October 30, 2020***

ABSTRACT

Internet fraud is a global issue and has posed challenges to the safe use of the cyberspace. The Cybercrime (prohibition and protection etc.) Act 2015 was enacted to regulate and guide the use of the internet in Nigeria, nonetheless, the challenge of internet fraud is on daily increase. This study focused on Cyber laws that have been advanced to abridge the menace caused by internet fraud. The cyber laws of other cyber secured countries are advanced through policies, approaches and practices of the enacted law by the citizens and concerned authorities. This has created a safe online environment that ensured security to users of the cyberspace. Adopting these strategies into the Nigerian Cyberlaw would invariably curb this challenging development in the country. The Committee on review of National Cybersecurity Policy and Strategy should enhance the Cybercrime Act 2015 by adopting advanced cyber laws practiced in other countries.

Keywords: *Cyber Laws; Internet fraud; Cybersecurity; Online Environment*

Introduction

Since the advent of ICT and communication networks, many aspects of everyday life have developed into a modern concept. This development created various opportunities and unhindered access to information. The use of internet has become a norm in Nigeria that 61.2% of the population are internet users (Internet World Stats, 2020). This created several opportunities such as blogging, web developing, research and publication and enhanced development in terms of monetary transaction and business. The Internet has been advantageous and has as well incurred threat to the cyberspace. Recently, Nigeria has been at the frontline of internet fraud and other sorts of cybercrimes in the globe. In 2019, the Federal Bureau of Investigation (FBI) indicated 80 people on internet fraud and 77 of them were Nigerians (BBC News, 2019). It has enveloped the nation with cyber threats and portrayed as a norm among the youths.

Internet fraud involves illegal activities carried out through the use of the internet, computer software and networks and includes fraudulent activities such as forgery, money laundering, and theft (Norwich University Online, 2019). The prevalence of this illicit attitude according to The Guardian (2017) is due to the quest for rich among Nigerian youths and the rich status of the dubbed Yahoo boys. This prevailing attitude has posed threat to the moral, intellectual and legit financial development of the youths. However, international and national efforts are put into place to curb the continuous occurrence of the internet through legislation and orders.

In most developed and developing countries, there is legal policy and rule on the use of the internet. The policies are made to guide internet users on the protection of private information to prevent illegal access. Cyber laws are legal actions imposed on grievances arising from e-business (Adeika, 2015). They are protracted for protection of online properties and safety businesses. These laws are practised and maintained in most countries and the users of the internet are ensuring security and safety. The uniqueness and innovation of the cybercrimes demand enhancement of the existing cyber law in Nigeria.

Recently, the Federal Government of Nigeria inaugurated a multi-stakeholder Committee to review the cybersecurity policy and strategy and enhance Cybercrime (prohibition and prevention) act 2015 to tackle the emanating (Ochayi, 2020). It is, therefore, recommended that the inaugurated committee members adopt the advanced cyber laws practices in other countries for a curb to the challenge of internet fraud in Nigeria.

Nigeria and the Threat of Internet Fraud

The emergence of ICT has created a prevailing online environment for storage and access to information. This situation enabled and enhanced intellectual and business growth by way of e-business as well as fraudulent activities. The fraudulent activities perpetrated through the use of the internet are a challenging incidence in the world particularly in Nigeria. The prevalence has caused the loss of millions from victims across the globe and has continued to violate the use of the internet in various ways ((Federal Bureau of Investigation, n.d). In 2018, 0.8% of the total global GDP was lost in the global economy as a result of internet fraud (McAfee, 2018). This steady occurrence of internet fraud in the Globe has become a major concern to Information Communication Technology and the security of e-business.

In Nigeria, the operation of financial fraud is dated back to the '90s when the fraudsters popularly known as 419ner's were using fax machines to defraud unsuspected foreigners and Nigerians (Ezea, 2017). They commanded respect because of the wealth at their disposal and were the big men and women in society. This occurrence persisted until recent times but exist in a different dimension known as internet fraud. Internet fraud involves defrauding victims in online space through the use of internet services with internet access (Federal Bureau of Investigation, n.d). Internet fraud as explained by Warf, (2018) is not a single distinctive crime, it includes illegal and illicit actions committed with the use of internet services and access. Internet fraud is rather regarded as a scam than theft because the victim voluntarily and knowingly provides the information, money, and property to the perpetrators (Brenner, 2009), and has been a threat to the online environment. The infringements in the use of the internet have instigated grievances in E-business and cybersecurity.

The perpetrators of internet fraud in Nigeria also known as the Yahoo Boys are role models among the Nigerian youths. They are at the disposal of wealth and assets and are the big boys among their mates. Recently, Nigerians are arrested in different countries for defrauding millions of dollar from victims. In 2019, The Federal Bureau of Investigation (FBI) indicted 77 Nigerians in an incidence described as the largest case of on-line fraud in US history (BBC News, 2019). Another incidence was the arrest social media celebrity known as "hushpuppi" in Dubai for defrauding around two million people of approximately half a billion dollars (Enahoro, 2020). Notwithstanding, millions of naira are lost in Nigeria through illegal access to confidential information of financial companies and individual. These incidences have threatened the reputation of being a Nigerian in the International market. It is worst that of the internet fraud methods is the "Nigerian letter fraud" (Federal Bureau of Investigation, n.d). Also, the report by Ezea (2017) and Enahoro (2020) indicated that despite the arrest and international assault and conviction of these fraudsters, the Nigerian youths are of increasing interest to the online criminal activity. Considering the rate of internet penetration in Nigeria between the year 2000 to 2020, a 61.2% increase was reported in the Internet World Stats (2020). The concern is then geared to what the future holds for Nigerian reputation in the international trade and online business transaction.

Nevertheless, the Internet enhances online transaction, access to information, and storage of crucial documents and intellectual properties. However, illegal and illicit use has instigated fear and insecurity to legal use. Invariably, the use of the internet has come to stay in innovative technology and ICT. Therefore, a curb to the emerging menace of internet fraud lies on enacted policy and orders that guides the use of internet and protection of users' information. Effective implementation of advanced law guiding the cyberspace in Nigeria would remove Nigeria from this menace caused by internet fraud.

Cyber Law in Nigeria

Cyberlaw is a policy and order guiding the cyberspace. Cyber laws are part of the legal system that deals with the internet and cyberspace activities. The Law is propounded to protect people's and organizations' confidential information from fraudsters on the internet. They are enacted to encourage the international exchange of goods and services in the online environment through transaction laws, data protection privacy law and consumer protection laws. Online transactions and e-business enhance the potential of international and national

transactions. The owners of e-business have assets of intellectual properties that are prospects to the interstate, national and international interests for which they have to protect (Adeika, 2015). Cyberlaw provides legal grievances to the potentialities of internet fraud. According to the United Nations Trade and Development (2015), Cyber laws had been enacted or pending adoption of a drafted law in 194member countries including Nigeria as of 2020. Cyber laws are grouped into different categories E-transaction Laws, Data protection privacy laws and consumer protection laws (United Nations Trade and Development, 2020). The cyber laws also include but not limited to Trademark, Servicemark, copyright, patents and trade secrets (Adeika, 2015).

Cyberlaw in Nigeria is noted to be in existence as early as 1990 under the criminal code Act of 1990. The criminal code Act posits that any type of stealing of funds in whatever form is an offence punishable under the act (Maitanmi, Ogunlere, Ayinde, & Adekunle, 2013). The Act specified in Chapter 38, section 418 that any representation made by words, writing or conduct, either in past or present, which representation is false and which the person making it knows to be false is a false pretence and is a punishable offence. Although the statement of the Act is not represented as cyberlaw, cybercrime offence characterizes the crime. Nevertheless, In 2015, the Federal Government of Nigeria enacted Cybercrime Act (Odumesi, 2015). The act prohibited any form of vandalization or crime against critical national information infrastructure, unlawful access to computer systems, online pornography, amongst others are punishable. The parts and sections of Cyber laws in Nigeria as written in Odumesi (2015) will be adopted for this study.

Part (1) Section (1) of the cybercrimes (prohibition, prevention etc.) Act 2015 provided the objectives of the Act which is to provide a legal and regulatory order for the protection of national information insecurity and promotion of cybersecurity in Nigeria.

Part (2) Section (3) and Section (4) of Cybercrimes (Prohibition, Prevention, etc.) Act 2015 explains the protection of critical national information infrastructure. This part of the Act specifies the designation of criminal activities towards the national information infrastructure such as computer systems/network

Part (3) Section (5) of Cybercrimes (Prohibition, Prevention, etc) Act 2015 explains offences against critical national information infrastructure thus;

1) Any person who with intent, commits any offence punishable under this Act against any critical national information infrastructure, designated under section 3 of this Act, shall be liable on conviction to imprisonment for a term of not more than 10 years without an option of fine.
2) Where the offence committed under subsection (1) of this section results in grievous bodily harm to any person, the offender shall be liable on conviction to imprisonment for a term of not more than 15 years without an option of fine.
3) Where the offence committed under subsection (1) of this section results in the death of the person(s), the offender shall be liable on conviction to life imprisonment.

The Significance of Advanced Cyber Laws in curbing Internet Fraud

Internet fraud is a global threat to the online environment. The incidence has caused lots of losses to the global GDP and attracted stern concerns from experts. The United Nations Trade and Development (2020) report on Cybercrime Legislation Worldwide showed that 79%, 5%, 13% and 2% of the member countries enacted legislation, drafted legislation, have no legislation and have no data respectively. The report showed that the majority of the member countries adopted cybercrime legislation while stating that Europe has the highest adoption rate, Asia and the Pacific has the lowest. The study carried out by (Analytics Insight, 2020) reported the top six countries with the best cybersecurity measures to include; USA, Russia, Isreal, China, Spain and Estonia. Nigeria was rated among the 11 countries with the worst cybersecurity.

The United States of America encounter cyberattacks on frequent occasion and are ranked best in cybersecurity. This is aligned to about 58% of the digital security organizations including better policies and practices situated to discover better tactics to battle most recent attacks. The government oftentimes, reassures transparency, productivity and development in regards to data security (The White House Washington, DC, 2018). In 2017, China adopted Cybersecurity to strengthen cybersecurity and national security. The law includes cybersecurity policies and regulations from different dimensions and fields (Analytics Insight, 2020). Among the best cybersecurity measures is the Estonian. After the cyber-attack in 2007, Estonia became world best in cyber-security-Knowledge. A cyber Coalition carried out by NATO (North Atlantic Treaty Organization) for three days pulled in more than 700 cyber defenders and supporting bodies such as legitimate specialists, government authorities, military personnel, and academic delegates (UNIDIR, 2020). The cyber laws and policy measures in these countries are advanced to suit the constant advancement in cybercrimes.

Also, the recent statistics by a privacy advocate and VPN expert, Bischoff (2020) showed that most countries have improved in cybersecurity with Denmark at the top of the list and Algeria the least. Nigeria was noted to improve from, 11th position to 20th position among countries with the least cybersecurity. This position is very poor as internet fraud has remained persistent and penetrative in society. The Denmark cyber law goals defined in the Danish Strategy for Cyber and Information strategy 2018-2021 were achieved through; (1) enhancement of its technological preparedness to protect essential societal functions against cyberattacks. (2) access by the citizens, businesses and authorities to the requisite knowledge and addressing the increasing level of cyber and information security challenges. (3) creating a clear division of roles and responsibilities among the authorities and business providing essential societal functions in the area of cyber and information security. This is can be achieved in Nigeria if effective adoption is made.

The place of the Nigeria cybercrime (protection, prevention etc.) Act 2015 is deficient in dealing with the rate of cybercrime. The Cybercrime (protection, prevention etc.) Act 2015 is similar to the cybercrime legislation of most other countries but differ in approaches. The newness and uniqueness of cybercrimes demand innovative and technological approach. Cybercrime in advanced countries depicts an innovative approach and responsibilities from the concerned authorities and bodies. In the analysis made by Ibekwe (2015), there are similarities in the between Nigerian Cybercrime (prohibition and prevention) Act 2015 and the Legal Framework on Cybercrimes in the UK. However, Investigations has shown that Nigeria is among the 15 countries with the highest number of internet

scammers (Bhalla, 2020). More so, in the recent news reported by (Ochayi, 2020) the Nigerian Federal Government inaugurated a multi-stakeholder committee to review the National Cybersecurity Policy and Strategy on the focus of enhancing the 2015 Act to address the challenges currently confronting nation including the emergence of new forms of criminality and terrorism perpetrated through the cyberspace. Therefore, it is a necessity that the review committee considers the adoption of advanced strategies and approaches capable of fighting internet fraud menace.

Conclusion and Recommendation

Advanced Cyber laws as obtainable in the advanced countries is an intriguing aspect of the global fight against cybercrimes. The existing cybercrime (prohibition and prevention) Act 2015 in Nigeria is constantly on defeat by the increasing rate of Cybercrimes and insecurity of the cyberspace. This has no doubt affected the economic, social and intellectual benefits in the use of cyberspace in Nigeria. Internet fraud is a major cybercrime among Nigerian youths and has remained a frequent occurrence in the daily news. It is, however, a global issue demanding curb from individual countries and has significantly been controlled in many countries. The Nigerian Cybercrime (prohibition and prevention) Act 2015 speculated to be under review should adopt the relevant advanced laws, policies, strategies and approaches that can solve the challenges perpetrated through internet fraud.

The uniqueness and newness of cybercrime demand a steady review of cyber laws with an innovative approach to the stated laws. This study, therefore, recommends that; the Federal Government should look beyond the protection of the national infrastructure in the online space to that of her citizens. The newly inaugurated committee on cybersecurity policy and strategy should consider and review advanced cyber law of leading countries in cybersecurity and adopt the necessary policies and strategies that can curb internet fraud in Nigeria. Individual companies and firms should secure their information and properties on the online space through the use of VPN (Virtual Privacy Network).

References

Adeika J. O. (2015). Cyberlaw - Standard and Legal Issues. *Researchgate*. Retrieved from https://www.researchgate.net/publication/280882159_Cyberlaw_-_Standard_and_Legal_Issues

Analytics Insight. (2020, February 18). *Top 6 countries with the best cybersecurity measures.* Retrieved from Analytics Insight: nalyticsinsight.net/top-6-countries-with-the-best-cyber-security-measures/#dat-menu

BBC News. (2019, September 23). *Letter from Africa: why Nigeria's internet scammers are 'role models'.* Retrieved from BBC News: https://www.bbc.com/news/world-africa-49759392

Bhalla, P. (2020, May 11). *Countries with Most Internet Scamming Fraudsters in eCommerce.* Retrieved from Shiprocket: https://www.shiprocket.in/blog/ecommerce-online-scamming-fraudsters-countries/

BIschoff, P. (2020, March 3). *Which countries have the worst (and best) cybersecurity?* Retrieved from Comparitech.

Brenner, S. W. (2009, January 16). *Cyberthreats: The emerging fault lines of the Nation States.* Retrieved from Oxford University Press: https://books.google.com/books?id=p31MCAAAQBAJ&pg=PT33&dq=internet+fraud+different+theft+voluntary#q=internet%20fraud%20different%20theft%20voluntary

Enahoro, E. (2020, June 30). *Nigeria: Internet Fraud and Get-Rich-Quick Mentality.* Retrieved from Daily trust: http://www.dailytrust.com.ng/

Ezea, S. (2017). *The prevalence of internet fraud among Nigerian youths.* Nigeria: The Guardian Saturday Magazine.

Federal Bureau of Investigation. (n.d). *Scams and Safety.* Retrieved from FBI: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud

Ibekwe, C. R. (2015). *The Legal Aspects of Cybercrime in Nigeria: An analysis with the UK Provisions.* Sterling: School of Law, University of Stirling.

Internet World Stats. (2020, March 31). *Internet Penetration in Africa 2020 - Q1 - March.* Retrieved from Internet world stats usage and population statistics: https://www.internetworldstats.com/stats1.htm

Maitanmi, O., Ogunlere, S., Ayinde, S., & Adekunle, Y. (2013). Cyber Crimes and Cyber Laws in Nigeria. *The International Journal Of Engineering And Science (IJES)*, 2319-1813.

McAfee. (2018). *The economic impact of cybercrime - no slowing down.* Retrieved from McAfree: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

Norwich University Online. (2019, November 8). *Career paths in information Security: What is Cyberlaw?* Retrieved from Norwich University Online: https://online.norwich.edu/academic-programs/resources/cyber-law-definition

Ochayi, C. (2020, October 6). *FG reviewing Cybersecurity Policy to tackle terrorism, Others.* Retrieved from Vanguard: www.vanguardngr.com/FG-reviewing-cybersecurity-policy-to-tackle-terrorism-others.hmm

Odumesi, J. (2015). *Nigeria's Cybercrimes (Prohibition, prevention etc) Act 2015 and critical National Infrastructure.* 10.13140/RG.2.1.4778.6726.

The White House Washington, DC. (2018, September). *The national cyber strategy of the United States of America.* Washington, DC: The White House Washington, DC.

UNIDIR. (2020). *Cybersecurity Policy.* Estonia, Estonia: UNIDIR Cyber policy portal.

United Nations Trade and Development. (2020, April 2). *Cybercrime Legislation Worldwide.* Retrieved from United Nations Trade and Development: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx

Warf, B. (2018, May 16). *The sage encyclopedia of the internet.* Retrieved from Sage: https://books.google.com/books?id=ED9XDwAAQBAJ&pg=PT1125&dq=internet+fraud+definition#q=internet%20fraud%20definition